RECEIVED
CENTRAL FAX CENTER
NOV 2 7 2006

REMARKS

This Amendment is responsive to the Final Office Action dated June 26, 2006. Applicant's amendment submitted August 25, 2006 was not entered. Applicant has submitted a Request for Continued Examination.

In this Amendment, Applicant has amended claims 1, 6, 7, 9, 11, 12, 13, 14, 17, 27, 35, 44, 45, 53, and 55. Applicant has canceled claims 8, 28, 40, 43, 54 and 56. Claims 1-4, 6, 7, 9-17, 27, 29-30, 35-39, 41, 42, 44-46, 53, and 55 are pending upon entry of this Amendment.

Claim Rejection Under 35 U.S.C. § 112

In the Final Office Action, the Examiner rejected claims 14 and 15 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner rejected claims 14 and 15 for being dependent on canceled claim 5. Applicant has amended claim 14 to properly depend from independent claim 1. Claim 15 is dependent on amended claim 14. Applicant submits that claims 14 and 15, as amended, particularly point out and distinctly claim the subject matter, as required by 35 U.S.C. 112, second paragraph. Applicant requests withdrawal of the rejections under 35 U.S.C. 112.

Claim Rejection Under 35 U.S.C. § 103

In the Final Office Action, the Examiner rejected claims 1, 3, 4, 6-11, 14, 15, 27, 28, 30, 35, 37-44 and 53-56 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,473,863 to Genty et al. ("Genty") in view of U.S. Patent No. 6,353,593 to Chen et al. ("Chen") in view of U.S. Patent No. 6,092,113 to Maeshima et al. ("Maeshima"). The Examiner also rejected claims 2 and 36 under 35 U.S.C. 103(a) as being unpatentable over Genty in view of Chen in view of Maeshima, and further in view of U.S. Patent Application No. 2003/0016679 to Adams et al. ("Adams"). In addition, the Examiner rejected claims 12, 13, 45 and 46 under 35 U.S.C. 103(a) as being unpatentable over Genty in view of Chen in view of Maeshima, and further in view of Jorgensen (US 2002/0099854). Finally, the Examiner rejected claims 16, 17 and 29 under 35 U.S.C. 103(a) as being unpatentable over Genty in view of Chen in view of Maeshima, and further in view of Shawcross (US 6,880,090).

Applicant respectfully traverses the rejections to the extent such rejections may be considered applicable to the claims as amended. The applied references fail to disclose or suggest the inventions defined by Applicant's claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

Applicants have amended independent claims 1, 18, 27, 35 and 53. Independent claim 1 now requires in response to the detected network attack, splitting the packet tunnel. Moreover, as recited by claim 1, splitting the packet tunnel is accomplished by selecting an intermediate network device that has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network. In this manner, claim 1 requires that, in response to a network attack, an intermediate network device is selected that has a network address that is not within the address space of the first local area network or the address space of the second local area network.

Amended claim 1 further requires establishing a first packet tunnel from the first local area network to the intermediate network device, establishing a second packet tunnel that originates from the intermediate network device to the second local area network, and communicating VPN traffic from the first local area network to the second local area network by redirecting the VPN traffic from the first local area network to the intermediate network device through first packet tunnel and forwarding the VPN traffic from the intermediate network device to the second local area network through second packet tunnel.

In this manner, in response to a network attack, an end-to-end packet tunnel is split and replaced by two tunnels that concatenated at an intermediate device outside the address space of the local area networks associated with the source and destination devices. This may provide numerous advantages.

For example, as explained on page 8 of the present application, a failover mechanism that simply replaces one VPN tunnel for another in response to a network attack may offer only limited protection. From the perspective of an external attacker, the new label assigned to the VPN flow by the failover process can take any value from among |S1|*|S2| possibilities, where S1 represents the address space of the source local area network and S2 represents the address space of the destination address space. The "address space diversity" refers to the quantity |S1|*|S2| that signifies the universe of possible values available to the randomized failover process for

reconfiguring a VPN flow label when its flow is under attack. This limited address space of |S1|*|S2| may allow the attacker to easily continue to attack the access link by spoofing other source addresses within this same address space.

In contrast, as described on pages 9-14 of the present application, embodiments of the invention address the issue of limited address space diversity by use of VPN tunnel splitting. When an attack on a VPN tunnel is detected, edge routers split the end-to-end tunnel between LANs into two or more concatenated tunnels. Thus, instead of a direct tunnel between edge routers that carries the VPN traffic, a VPN tunnel is dynamically created using two or more tunnels that are concatenated at one or more tunnel concatenation devices (TCDs). Consequently, the VPN flow from a source edge router to a destination edge router is redirected over a new tunnel to an intermediate network device and the forwarded to the destination by a second tunnel. The intermediate network device can be another edge router potentially owned by a third party with which an enterprise has established a trust relationship.

As explained in the present application, conceptually, tunnel splitting may be viewed as facilitating the reconfiguration of the label of the flow from one LAN site to another without limiting the address space diversity that is available for performing this reconfiguration. By use of intermediate devices that have network addresses different from the address spaces associated with the source and destination local area networks, increased address space diversity can be obtained. Thus address space diversity with tunnel splitting is not limited to |S1|*|S2| possibilities, and instead is (size of the unicast IP address space)^2 *(number of source ports)*(number of destination ports) or approximately $56*10^{27}$. Thus, embodiments of the invention greatly increase the survivability of the VPN service compared to label reconfiguration with direct tunnels that terminate within the same source and destination address space.

Genty in view of Chen and Maeshima fail to teach or suggest the elements of claim 1. Genty in view of Chen describes establishing the secondary tunnel and abandoning the original tunnel upon detecting a network attack. However, this technique suffers from the exact problem described by the Applicant, i.e., the problem of limited address space diversity. Any new end-to-end tunnel created in Genty would be sourced and terminated within the same address spaces as the source and destination devices and, therefore, would continue to be highly susceptible to address spoofing. Maeshima only adds the notion of reserving bandwidth for the end-to-end

tunnels on a network, including the newly established tunnel. Neither Maeshima nor any of the other cited references overcome these deficiencies.

Furthermore, many of Applicant's dependent claims are directed to techniques by which the source device and the destination device cooperate so as to select an intermediate device and split the tunnel in response to a network attack. Claim 6, for example, recites exchanging a set of available network addresses between the source network device and the destination network device, wherein the set of available network addresses correspond to a plurality of intermediate network devices. Claim 9 requires, upon detecting the network attack, sending a message from the destination network device to the source network device instructing the source network device to establish the first packet tunnel with the intermediate network device. Claim 10 requires sending the message over a secure signaling channel. None of the references, either singularly or in combination, teach or suggest these elements.

For these or other reasons, the references fail to establish a prima facie case for non-patentability of Applicant's claims 1-4, 6, 7, 9-17, 27, 29-30, 35-39, 41, 42, 44-46, 53, 55 and 56 under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

CONCLUSION

All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed agent to discuss this application.

Date:

November 27, 2006

By:

Name: Kent J. Sieffert
Reg. No.: 41,312

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102